



## OIT 62.902: Threat Detection

**Responsible Executive:** Information Security Officer  
**Responsible Office:** Office of Information Technology  
**Related Policy:**  
**Approved-On Date:** 4/19/2011  
**Effective Date:** 7/1/2011  
**Revision Date:** 4/11/2011

### I. Policy Statement

Threat Detection addresses protection of IT systems and information by preparing for and responding to information security incidents.

### II. Purpose

The Threat Detection policy identify the requirements for implementing intrusion detection and prevention

### III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

### IV. Requirements

The University shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:

1. Designate an individual responsible for the University's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
2. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
3. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.
4. Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.
5. Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

6. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.

## **V. Violations**

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

## **VI. Interpretation**

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.